IN THE CLAIMS:

1. (Previously Presented) In a digital scanner, a method for secure document transmission, the method comprising:

creating computer text files, called profiles, each profile having an address field and an encryption field;

storing the profiles in a directory;

at a scanner device user interface, selecting a profile from the directory;

accepting a physical medium document;

scanning the document;

encrypting the scanned document in response to the encryption field of the selected profile; and,

sending the encrypted document to a destination in response to the address field of the selected profile.

2. (Previously Presented) The method of claim 1 wherein sending the encrypted document to the destination includes sending the encrypted document to a network-connected destination in response to the address field of the selected profile.

3. Canceled

4. (Previously Presented) The method of claim 1 further comprising:

assigning each profile to a corresponding destination; and,

wherein selecting a profile includes:

selecting a destination; and,

using the profile assigned to the selected destination.

5. (Previously Presented) The method of claim 1 wherein selecting a profile includes selecting a profile having an address selected from the group including email addresses and file transfer protocol (FTP) addresses.

6. (Previously Presented) The method of claim 1 wherein selecting a profile includes selecting a profile having an encryption field selected from the group including symmetric and asymmetric (public) keys.

7. (Original) The method of claim 6 wherein selecting a profile includes selecting a profile having an asymmetric key; and,

wherein creating profiles includes storing public keys in the created profiles.

8. (Original) The method of claim 6 wherein selecting a profile includes selecting a profile having a symmetric key; and,

wherein creating profiles includes storing symmetric keys in the created profiles.

9. (Previously Presented) The method of claim 1 wherein creating profiles includes creating profiles for a plurality of user groups;

the method further comprising:

generating a plurality of passwords for the corresponding plurality of user groups; and,

wherein storing the profiles in a directory includes storing profiles in a profile directory, in response to the generated password.

10. (Previously Presented) The method of claim 1 wherein selecting a profile includes selecting a profile having a link to a certification authority storing a public key; and,

wherein encrypting the document using the encryption field from the selected profile includes using the public key signed by the certification authority to encrypt the document.

11. (Original) The method of claim 7 wherein encrypting the document using the encryption field from the selected profile includes:

generating a random session key;

encrypting the document with the session key using a symmetric algorithm;

encrypting the session key with an asymmetric algorithm using the selected profile public key; and,

wherein sending the encrypted document to the address from the selected profile includes sending the encrypted session key.

12. (Original) The method of claim 6 wherein creating profiles includes creating a profile with a plurality of addresses and a corresponding plurality of public keys;

wherein encrypting the document includes generating a single encrypted document using an asymmetric algorithm; and,

wherein sending the encrypted document includes sending the single encrypted document to each of the plurality of addresses in the profile.

13. (Previously Presented) In a digital scanner, a method for secure document transmission, the method comprising:

storing computer text files, called profiles, in a directory of a scanner device, each profile having an address field and an encryption field;

at a user interface associated with the scanner device, selecting a profile from the directory;

scanning a document;

encrypting the scanned document in response to the encryption field of the selected profile; and,

sending the encrypted document from the scanner device, to a network-connected destination, in response to the address field of the selected profile.

14. (Previously Presented) A digital scanner secure document transmission system, the system comprising:

a profile directory having a user interface for selecting computer text files, called profiles, each profile including an encryption field and an address field;

a document scanner to accept physical medium documents, create scanned documents, and encrypt the scanned documents in response to selected profile encryption fields; and,

a network interface for transmitting the encrypted documents to a destination in response to the profile address field.

15. Canceled

16. (Previously Presented) The system of claim 14 further comprising:

a memory for storing the profiles; and,

wherein the profile directory has an interface for creating profiles having an address field and an encryption field;

17. (Original) The system of claim 16 wherein the profile directory has an interface for accepting destinations and assigning each profile to a corresponding destination; and,

wherein profiles are selected from the profile directory in response to entering the destination.

18. (Original) The system of claim 16 wherein the profile directory supplies selected profiles having an address selected from the group including email addresses and file transfer protocol (FTP) addresses.

19. (Original) The system of claim 16 wherein the profile directory supplies selected profiles having an encryption field

selected from the group including symmetric and asymmetric (public) keys.

20. (Original) The system of claim 19 wherein the profile directory supplies selected profiles having an asymmetric key; and,

wherein the memory stores the public keys corresponding to each profile.

21. (Original) The system of claim 19 wherein the profile directory supplies selected profiles having a symmetric key; and,

wherein the memory stores the symmetric keys corresponding to each profile.

22. (Original) The system of claim 16 wherein the profile directory has an interface for generating passwords, the profile directory creating profiles for a plurality of user groups in response to the generated passwords.

23. (Original) The system of claim 16 further comprising:

a certification authority storing public keys;

wherein the profile directory supplies a selected profile having a link to the certification authority;

wherein the network interface negotiates with the certification authority for a public key corresponding to the selected profile; and,

wherein the document scanner uses the public key signed by the certification authority to encrypt the document.

24. (Original) The system of claim 20 wherein the document scanner generates a random session key and encrypts the document with the session key using a symmetric algorithm;

wherein the document scanner encrypts the session key with an asymmetric algorithm using the selected profile public key; and,

wherein the network interface transmits the encrypted session key with the encrypted document.

25. (Original) The system of claim 19 wherein the profile directory supplies a selected profile with a plurality of addresses and a corresponding plurality of public keys;

wherein the document scanner encrypts the document into a single encrypted document using an asymmetric algorithm; and,

wherein the network interface sends the single encrypted document to each of the plurality of addresses in the selected profile.

26. (Previously Presented) A digital scanner secure document transmission system, the system comprising:

a directory having a user interface for selecting an address field cross-referenced to an encryption field;

a document scanner to accept physical medium document, create a scanned document, and encrypt the scanned document using the cross-referenced encryption field; and,

a network interface for transmitting the encrypted document to a destination using the selected address field.

27. (Previously Presented) In a digital scanner, a method for secure document transmission, the method comprising:

cross-referencing an address field to an encryption field;

storing the cross-referenced fields in a directory;

at a scanner device user interface, selecting an address from the directory;

accepting a physical medium document;

scanning the document;

encrypting the scanned document using the cross-referenced encryption field; and,

sending the encrypted document to a destination using the selected address field.